Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In re Digital Broadcast Copy Protection	MB Docket No. 02-230

COMMENTS OF THE NATIONAL CABLE & TELECOMMUNICATIONS ASSOCIATION

Paul Glist
Cole, Raywid & Braverman, L.L.P.
1919 Pennsylvania Avenue, N.W.
Suite 200
Washington, D.C. 20006
(202) 659-9750

Daniel L. Brenner
Neal M. Goldberg
Michael S. Schooler
National Cable & Telecommunications Association
1724 Massachusetts Avenue, N.W.
Washington, D.C. 20036-1903
(202) 775-3664

December 6, 2002

TABLE OF CONTENTS

Before the
FEDERAL COMMUNICATIONS COMMISSION
Washington, DC 20554

In re Digital Broadcast Copy Protection	MB Docket No. 02-230

COMMENTS OF THE NATIONAL CABLE & TELECOMMUNICATIONS ASSOCIATION

The National Cable & Telecommunications Association ("NCTA") hereby submits its comments in support of the Federal Communications Commission's efforts to facilitate digital broadcast copy protection, as described in the Notice of Proposed Rulemaking ("NPRM" or "Notice") adopted on August 8, 2002.

NCTA is the principal trade association of the cable television industry, representing operators serving over 90 percent of the nation's cable customers. These companies also provide high-speed access to the Internet and other services. NCTA's members also include more than 200 cable program networks, as well as companies that provide equipment and services to the industry.

SUMMARY

The Commission has previously recognized that installing the tools for digital copy protection is essential in the digital transition. Representatives of NCTA and other cable interests actively participated in the Broadcast Protection Discussion Group ("BPDG") discussions and the development of its proposal that over-the-air television receivers should read and respect embedded digital instructions in digital television ("DTV") broadcasts that instruct the devices not to engage in unauthorized redistribution

of programming over the Internet. NCTA supports the concept of a broadcast flag with the limited purpose of restricting appropriately-marked digital broadcasts against Internet retransmission, as proposed in the Notice.

In moving forward with a "broadcast flag," the Commission should take care to preserve the flexibility and variety in secure consumer choice technology tools and paths for rapid innovation. Any rules adopted should allow different media to protect against Internet retransmission of digital broadcast signals through different techniques that achieve the same functional result, just as different solutions have evolved for different media today. In particular, it is not necessary to embed the Redistribution Control descriptor when a broadcast signal is managed at the cable headend, so long as the appropriate instruction is delivered to a digital television receiver or other device connected to the cable system.

Maintaining the flexibility to develop a secure cable home domain will also allow greater dissemination of programming within the home for private home use. Any rules should also accommodate the ability to innovate and rapidly deploy new secure outputs and interfaces, without compromising existing secure consumer choice technology solutions. The selection and expansion of authorized digital output protection technologies and authorized recording methods should be the result of a fair, reasonable and nondiscriminatory process using a combination of both "market-based" criteria and technical criteria. The rules should also be sufficiently flexible so that publishers and distribution media may promptly respond to consumer reaction, hacking, and similar market changes.

The Commission should also assure that the proposed three bytes comprising the Redistribution Control descriptor be limited and used solely to signal consumers' over-the-air television receivers not to engage in unauthorized redistribution of digital broadcast programming over the Internet, and not for other purposes.

I. BACKGROUND

Making copies of over-the-air broadcast programming has been widespread since the broad dissemination of the analog videocassette recorder. But despite initial apprehensions, any adverse effects of such copying have been constrained in practice by the degradation of analog copies; by the new business opportunities home copying devices created for program owners; and, despite the growth of the Internet, by the relative scarcity of analog-to-digital converters and bandwidth constraints of most home Internet connections. With a wider transition to digital broadcasting and digital television receivers, concerns over an adverse impact on programming available to broadcasters have surfaced again.

Cable operators must negotiate with content providers for access to programming. For high-value digital programming to be made available to cable operators, program suppliers need the confidence that the copy protection infrastructure of cable systems (and the devices attached to them) are designed with tools that can manage against unauthorized copying and redistribution of that programming. The cable industry has responded by designing such tools into its systems and specifications. For similar reasons, direct broadcast satellite ("DBS") providers have built similar tools into their receivers. On the Internet, content providers have engaged in well-publicized efforts to

prevent unauthorized peer-to-peer dissemination of motion pictures, and some are now gradually adopting secure consumer choice technology solutions for authorized viewing of motion pictures over the Internet.

In the broadcasting context, programming is normally released within carefully defined time windows, with territorial restrictions, and with an eye to earning subsequent revenues from syndication. As a result, broadcasters are also justified in their desire to have sufficient tools to maintain competitive access to high-value digital programming that might otherwise migrate to other technological platforms. Indeed, the Commission has specifically endorsed respect for such technological measures as essential in the digital transition.[1]

The "broadcast flag," which is the subject of the present docket, is one part of this widespread effort to implement appropriate solutions. But it is a narrow one. The proposed broadcast flag does not restrict copying of broadcast programming for non-commercial home use. This docket concerns only the unauthorized redistribution over the Internet of digital broadcast programming received by home broadcast receivers, and only the DTV programming marked for such protection.

[1] *See Commercial Availability of Navigation Devices*, Further Notice of Proposed Rulemaking and Declaratory Ruling, 15 FCC Rcd 18199 at ¶ 15 (2000) ("Unlike the analog context, digital technology affords users the ability to make an unlimited number of virtually perfect copies of digital content. Also unlike the analog context, copyright holders of digital content possess the ability to prevent misuse of copy-protected material through methods not previously available. Through the use of contractual licensing requiring consumer electronics manufacturers to install certain copy protection technology in their equipment in exchange for access to desirable digital content, copyright holders will be able to control, through the insertion of coded instructions in the digital stream, whether such equipment will allow consumers to make one copy, unlimited copies, or prohibit copying altogether of digital content received from an MVPD.")

II. THE PROPOSED BROADCAST FLAG

What is technically required to protect against unauthorized redistribution over the Internet of digital broadcast programming is fairly straightforward: television receivers need to be instructed not to output the signal to the Internet; and other devices that may be connected to such receivers, or that receive over-the-air recordings of digital broadcast programming, need to read and respect similar instructions. The instruction can, and should be, quite simple: a single bit can be set to "on" or "off" to signal protection.[2]

The proposed broadcast flag is one of many secure consumer choice solutions that have been developed in the marketplace. Different solutions have been tailored to DVDs, cable television, music, Internet content, and computer software, to name a few. DVDs of motion pictures rented from video and DVD rental companies are embedded with Content Protection for Recordable Media ("CPRM") anti-copying instructions. Cable systems will receive and decrypt programming off a satellite, arrange it into compressed digital channels, group those channels into tiers, and secure reception with conditional access instructions that are signaled to the home through out-of-band channels separate from the channel over which the video itself is delivered. A recently-announced secure consumer choice technology from Microsoft allows Warner Bros. to offer Internet

[2] The proposed Redistribution Control descriptor is sufficient to signal the presence or absence of the flag, but should be limited to a single binary bit to accomplish that function. The complete Redistribution Control descriptor consists of 24 bits: one 8-bit integer that identifies the descriptor, one 8-bit integer that specifies the length of the information to follow, and 8 bits of "optional additional information that may be defined in the future." Amendment No. 3 to Revision A of ATSC Standard: Program and System Information Protocol for terrestrial Broadcast and Cable Doc. A/65A – (31 May 2000), Doc. T3-556, April 1, 2002. As explained below, the Commission should make certain that the unused bits and the additional 8-bit integers are removed or limited to signaling a restriction against Internet retransmission.

delivery of the film "Harry Potter and the Sorcerer's Stone" viewable for 24 hours.[3] Liquid Audio offers Internet promotion services for music, such as real-time streams and free or time-limited downloads, which provide music content owners and retailers with a method to promote new artists and generate on-line sales.[4] Universal Studios Pay-Per-View recently announced a four-month trial with CinemaNow, Inc. for downloading and streaming movies through CinemaNow's video-on-demand web site.[5] This is just the tip of the iceberg of the variety of secure consumer choice technology available now or under development.[6]

For business-to-business relationships, intellectual property rights traditionally rely upon business obligations, exempting professional equipment from the mandatory standards applied to consumer electronics. For example, Section 1201(k) of the Digital Millennium Copyright Act[7] exempts professional recorders used in the media business from the copy protections consumer electronics devices must employ.

It is clear that all the various forms of content and media do not, and should not, use the same technologies. In the technologically complex and rapidly developing area of secure consumer choice technology, a "one size fits all" approach is unwise and would likely be counter-productive.

---

[3] *See* http://www.siliconvalley.com/mld/siliconvalley/4037936.htm.

[4] This service is described in detail on Liquid Audio's web site at: http://www.liquidaudio.com/services/promotions/index.asp.

[5] The trial will include first-run titles such as "Big Fat Liar," "The Scorpion King" and "Brotherhood of the Wolf," as well as catalog titles such as "Erin Brockovich" and "Psycho." *See* http://www.cinemanow.com/about/press_article.asp?pr_id=58.

[6] A list of recent vendor developments can be found at: http://www.giantstepsmts.com/DRM%20Watch/vendors.htm.

III. THE BPDG AND ITS "FINAL REPORT"

As the Commission has noted, the Broadcast Protection Discussion Group was a discussion group that entertained comments on the broadcast flag from a large number of interested programmers, distributors, broadcasters and consumer electronics ("CE") manufacturers.[8] As a participant, however, NCTA would like to clarify what the BPDG set out to accomplish and what it delivered in the Final Report of the Co-Chairs issued June 3, 2002 (the "BPDG Report").

The BPDG was a subgroup formed under the Copy Protection Technical Working Group ("CPTWG"). However, the BPDG was an informal discussion vehicle without a defined process for measuring "consensus" among the participants. Under past CPTWG procedures, such as the development of DVD protection standards, such discussions move to a more formal body or process under which participation and the development of consensus is more rigorously crafted. Partly because of these constraints, and partly because of the BPDG's interest in providing timely reports to interested members of Congress, the BPDG Report was neither complete on the technical side nor did it represent a "consensus" among all participants. This is why the BPDG Report is very narrow in what it actually reports, why it reflects some significant disagreements between CE manufacturers,[9] and why it includes a wide assortment of noted concerns that were unresolved.[10]

---

[7] 17 U.S.C. § 1201(k)(3).

[8] NPRM at ¶ 2.

[9] *See, e.g.*, BPDG Report §§ 5.6, 5.7.

[10] *See,* BPDG Report Section 5 (points as to which no consensus was reached) and Section 6 (unresolved matters).

The conclusion of the BPDG Report, with which NCTA agrees, is that consumer electronics that can receive over the air broadcast signals should read and respect embedded digital instructions in DTV broadcasts that instruct the devices not to engage in unauthorized redistribution of programming over the Internet.[11] Among the significant unresolved technical issues in the Report are (1) the exemption for professional equipment;[12] (2) preserving appropriate means for innovating and adding "approved outputs;"[13] and (3) use of the broadcast flag within the cable home domain.[14]

Participants in the BPDG discussions agreed that there should be a professional equipment exemption. [15] For example, it is not necessary to embed the Redistribution Control descriptor when a broadcast signal is managed at the cable headend, so long as the appropriate instruction is delivered to a digital television receiver connected to the cable system. However, the language for such an exemption never found its way into the BDPG Report.

Participants in the BPDG discussions were divided on how "outputs" are to be approved.[16] At any given moment, different interfaces are in vogue and use different security. Only a few years ago, typical interfaces would be Variable Graphics Array

[11] BPDG Report Tab C – "Requirements for the Protection of Unencrypted Digital Terrestrial Broadcast Content Against Unauthorized Redistribution." Section 3.5 of BPDG Report describes this document as "the primary work product of the BPDG."

[12] BPDG Report Tabs D and E – alternative X.2 riders prepared by certain MPAA and CE/IT BPDG representatives, at footnote 1 ("We *anticipate* that an appropriate provision would be crafted so as to exempt these requirements from applying to products that are specifically intended for professional video and broadcast use.") (emphasis added).

[13] BPDG Report § 6.6.

[14] BPDG Report §§ 5.1, 6.2.

[15] BPDG Report § 4.12.

[16] BPDG Report § 6.6.

("VGA") or component analog (three plugs of different colors). Today, however, digital interfaces would include the IEEE 1394 connector (a physical plug for digital recording devices) and the Digital Video Interface ("DVI") connector that permits delivery of an uncompressed digital signal to the television. A modification to DVI has also recently been proposed, called High Definition Multimedia Interface ("HDMI"), which adds an audio channel. All parties have an interest in assuring that a new interface fully supports applicable copy protections. Thus, a process should be established that would accommodate the ability to innovate and rapidly deploy new interfaces, without compromising existing solutions. The BPDG was unable to find this balance, and so reported only two possible methods.[17]

Also unresolved was the handling of the cable home domain, or any home domain.[18] Cable operators are increasingly involved in managing home domains for consumers who wish to share modems, printers and home gateways, and who wish to move programming around the home network for private home use. As these home domains are secured, they become increasingly extensions of the cable headend, and may well utilize consumer choice technologies (within the secure network) that are different from – but equally effective as – the proposed broadcast flag.

IV. THE ROLE OF THE COMMISSION

NCTA agrees with the concept of a broadcast flag with the limited purpose of restricting appropriately-marked digital broadcasts against Internet retransmission, as

[17] BPDG Report § 3.6, Tabs D and E – alternative X.2 riders prepared by certain MPAA and CE/IT BPDG representatives.

[18] BPDG Report §§ 5.1, 6.2.

proposed in the Notice. Against the backdrop of multiple secure consumer choice technologies and unresolved issues in the BPDG Report, however, any government effort to craft regulations based principally upon the BPDG Report should proceed with caution. (NCTA assumes for purposes of these Comments that the Commission has – or will have – the authority to craft regulations regarding digital broadcast copy protection either under existing law or through additional legislation.)

A. The Commission Should Maintain Flexibility in Secure Consumer Choice Technologies.

Any government regulation in this area should be crafted so as to not frustrate the use of techniques that achieve the same result but in ways optimized for the particular technology. Broadcast programming can flow through a variety of distribution media – broadcast tower, satellite, cable or terrestrial wireless – before it reaches a consumer's television receiver. So long as each medium has the performance obligation to instruct the receiver not to engage in unauthorized retransmission over the Internet, each medium will be able to adopt techniques best suited to its technology.

A broadcaster would naturally have an incentive, even without government regulation, to encode its programming in the location and with the technical instruction that can be read directly by the television receiver. On the other hand, intermediary distributors of broadcast content (such as cable or DBS) often download, multiplex, translate, and/or modulate the content onto specific transportation mediums. Along this route, a wide variety of techniques might be employed. A cable operator, for example, might translate the embedded code into an out-of-band signal for carriage within its network, as long as it outputs a program with the proper instruction placed in the position

expected by the television receiver. A cable operator managing a home domain could go further and create a "reverse firewall" to keep the programming within the secure home domain and protect against redistribution over the Internet. Either approach would accomplish the required result, but could utilize techniques that are optimized for the medium, and thereby avoid needless costs. Just as different solutions have evolved for different media today, different media should be able to protect against Internet retransmission through different techniques that secure the same functional result.

B. The Commission Should Protect Paths for Innovation.

Government regulation should also be crafted so as not to frustrate innovation. As the Commission well knows, the pace of innovation in the communications industry is relentless. Time and again, market forces have been proven to deliver greater innovation and choice to consumers than regulatory mandates. The communications industry, and cable television in particular, have an astounding record of innovation. Cable operators have invested more than $65 billion, or over $1,000 per subscriber, in private risk capital since 1996 to upgrade systems to deploy higher quality television programming and advanced two-way broadband services to customers. Many of the capabilities possible with these newly upgraded networks are not yet developed, or even imagined. On the home network side, just as VCRs burst on the scene twenty years ago and entirely changed the economics of the entertainment industry, DVD technology and personal video recorders ("PVRs") such as SONICblue's ReplayTV and TiVO are growing at a very strong pace. Indeed, DVD penetration is now at 30

percent,[19] and is quickly supplanting analog VHS tapes as the standard in the video retail and rental industry. In light of the opportunities created by such rapid innovations, the Commission should craft any regulations in this area with an eye towards permitting and encouraging continued innovation.

C. The Commission Should Devise a Reasonable, Non-Discriminatory Process for Defining Authorized Digital Output Technologies and Recording Methods.

The selection and expansion of authorized digital output protection technologies and authorized recording methods should be the result of a fair, reasonable and nondiscriminatory process for obtaining approval of technologies for inclusion on the BPDG Report's "Table A."[20] The process must also be clearly defined, rapid, inclusive of all parties, and include definite timetables for approval and appeal procedures before a neutral decision-making body. Business models and technology solutions in video distribution and home networking move at a fast pace; likewise, the process for approval of technologies must move quickly.

A combination of both "market-based" criteria (such as the proposal set forth at Tab F of the BPDG Report) and technical criteria (such as the proposal set forth at Tab G of the BPDG Report) would be the most effective approach.

D. The Commission Should Consider the Impact of Regulations on the Cable Home Domain.

Maintaining the flexibility to develop the secure cable home domain can produce great consumer benefits: it invites innovation to allow greater dissemination of

[19] "DVD a Hit at Home-Theater Box Office," CNET News.com, July 1, 2002 (citing data from the market research firm NPD Techworld).

programming within the home for private home use. Such an approach also decreases the risk of abridging consumer home use. By contrast, the adoption of a government mandate that a selected secure consumer choice technology be imposed at the point of demodulation could very well frustrate such innovation and benefits to consumers.

E. Regulations Should Permit Rapid Deployment of Secure Consumer Choice Technology Improvements.

Government rules should be able to permit rapid deployment of secure consumer choice technology improvements. In the past, software suppliers, for example, had to specifically revise their software security to make it more suited to PC consumer usability. Likewise, music publishers recently discovered the need to revise their security to make CDs playable on consumers' existing players. Government rules should be sufficiently flexible so that publishers and distribution media may promptly respond to consumer reaction, hacking, and similar market changes.

F. Any Mandated Solution Should Be Limited In Scope.

As proposed in the Notice, the scope of the proposed broadcast flag solution should be limited to what is intended and needed to protect content providers' interests against unauthorized Internet retransmission of their high value content. The proposed broadcast flag, the Redistribution Control descriptor, consists of three bytes (24 bits) of data, including eight bits for "optional additional information that may be defined in the future."[21] This is more capacity than is required to instruct the receiver to protect against

---

[20] BPDG Report Tab C – Requirements for the Protection of Unencrypted Digital Terrestrial Broadcast Content Against Unauthorized Redistribution.

[21] Amendment No. 3 to Revision A of ATSC Standard: Program and System Information Protocol for Terrestrial Broadcast and Cable, Doc. A/65A – (31 May 2000), Doc. T3-556, April 1, 2002.

unauthorized redistribution over the Internet. In order to avoid unintended uses (or abuses) of such a dataflow, which flows directly to subscriber equipment, the Commission should include a limitation on any extraneous uses of the broadcast flag. The proposed Redistribution Control descriptor should be confined to the specific bits needed for that purpose, and its use should be limited to that specific function.

CONCLUSION

Broadcasters, like other distributors of digital content, are justified in their desire to have sufficient tools to maintain competitive access to high-value digital programming that might otherwise migrate to other technological platforms. But in considering moving forward with a "broadcast flag," the Commission should take care to preserve the flexibility and variety in secure consumer choice technologies and paths for rapid innovation. Any rules adopted should allow different media to protect against Internet retransmission of digital broadcast signals through different techniques that achieve the same functional result, just as different solutions have evolved for different media today. In particular, it is not necessary to re-embed the Redistribution Control descriptor when a broadcast signal is managed at the cable headend, so long as the appropriate instruction is delivered to a digital television receiver connected to the cable system. Maintaining the flexibility to develop a secure cable home domain will also allow greater dissemination of programming within the home for private home use.

Any rules should also accommodate the ability to innovate and rapidly deploy new outputs and interfaces, without compromising existing solutions. The selection and expansion of authorized digital output protection technologies and authorized recording methods should be the result of a fair, reasonable and nondiscriminatory process using a

combination of both "market-based" criteria and technical criteria. The rules should also be sufficiently flexible so that publishers and distribution media may promptly respond to consumer reaction, hacking, and similar market changes. The Commission should also assure that the proposed three bytes (24 bits) comprising the Redistribution Control descriptor be limited and used solely to signal consumers' over-the-air television receivers not to engage in unauthorized redistribution of digital broadcast programming over the Internet, and not for other purposes.

Respectfully submitted,

_____

Paul Glist
Cole, Raywid & Braverman, L.L.P.
1919 Pennsylvania Avenue, N.W.
Suite 200
Washington, D.C. 20006
(202) 659-9750
pglist@crblaw.com

Daniel L. Brenner
Neal M. Goldberg
Michael S. Schooler
National Cable & Telecommunications Association
1724 Massachusetts Avenue, N.W.
Washington, D.C. 20036-1903
(202) 775-3664

December 6, 2002